U. S. Department of Education

Office of the Chief Information Officer

Information Resources Management (IRM)

Strategic Plan

FY 2014 – 2017

Final

August 31, 2015

Contents

1 Introduction 6

2 IRM Goals 7

3 Goal One: Portfolio Alignment 8

3.1 Department Alignment 8

3.1.1 Department Strategic Plan 8

3.1.2 Segment Architecture 10

3.1.3 Value Measurement Methodology (VMM) 12

3.2 Federal Alignment 13

3.2.1 Digital Government Strategy 14

3.2.1.1 Implementing the Digital Government Strategy 14

3.2.1.2 Information Centric 15

3.2.1.3 Shared Platform 17

3.2.1.4 Customer Centric 19

3.2.1.5 Security and Privacy 21

3.2.2 Federal Data Center Consolidation 23

4 Goal Two: Technology Services 23

4.1 Current Services 24

4.2 Future Services 25

4.2.1 CIO's Innovation Agenda 27

4.2.1.1 Access Anywhere Computing 27

4.2.1.2 OCIO Support Services 27

4.2.2 Common Enabling Services (CES) 28

4.2.3 Commodity IT and Shared Services 30

4.2.3.1 Maturing the IT portfolio 30

4.2.3.2 Use of savings resulting from consolidations of Commodity IT 31

4.2.3.3 Maximizing use of inter- and intra-agency shared services 31

4.2.3.4 Continuity of operation for mission critical applications 32

4.2.4 Cloud Computing 32

4.2.5 Data Analytics Strategy Initiatives 33

4.2.5.1 Data Analytics at Department of Education 33

4.2.5.2 Creating a Data-Driven Culture at the Department of Education 34
4.2.5.3. Efforts at the Department to Establish a Data-Driven Culture 34
4.2.5.4. Data Analytics Technology 35
4.2.6 Cybersecurity Initiatives 36
4.2.6.1 HSPD-12 36
4.2.6.2 TIC 36
4.2.6.3 CM 37
4.2.7 IPv6 38
4.2.8. Electronic Stewardship 38
5 Goal Three: Information and Technology Management 38
5.1 IT Governance Structure 38
5.1.1 Enterprise Architecture Program Office (EAPO) 39
5.1.2 Investment and Acquisition Management Team (IAMT) 39
5.2 Key Department Contributors to the IRM Governance Process 40
5.2.1 IT Acquisition (Procurement) 40
5.2.2 Regulatory Information Management 40
5.2.3 Information Assurance Services (IAS) 40
5.2.4 Information Technology Services (ITS) 40
5.2.5 Accessibility 41
5.2.5.1 Creating a diverse work environment for individuals of all abilities 41
5.2.5.2 Building workforce skills to support and enforce Section 508 requirements 41

Revision History

Date	Version	Updates	Section #
8/13/15	FY14-FY17	Updated the Document Purpose section	
8/13/15	FY14-FY17	Inserted a bullet in the Introduction section	1
8/13/15	FY14-FY17	Removed bullets under IRM Goals section	2
8/13/15	FY14-FY17	Removed Strategic Goals table	3.1.1
8/13/15	FY14-FY17	Removed section and added it to section 3.2.1	3.2.3
8/13/15	FY14-FY17	Updated section, removed graphic	4.2.1.1
8/13/15	FY14-FY17	Updated the CES table, removed repeting rows and condensed Data Analytics para	4.2.2
8/13/15	FY14-FY17	Removed Current cloud Services table	4.2.4
8/13/15	FY14-FY17	Updated section, condensed paragraphs, removed graphics and removed repeating rows in table	4.2.5
8/13/15	FY14-FY17	Updated section, removed table	4.2.6
8/13/15	FY14-FY17	Updated Information Technology Services (ITS) section	5.2.4
8/13/15	FY14-FY17	Removed Human Capital Management section	5.2.5
8/13/15	FY14-FY17	Updated Accessibility section	5.2.6
4/22/15	FY14-FY17	Added Future Cloud Services table	4.2.4
4/22/15	FY14-FY17	Added a new section on Data Analytics	4.2.5
4/22/15	FY14-FY17	Update section (Cyber Security Initiatives)	4.2.6
4/22/15	FY14-FY17	Updated section (IPv6)	4.2.7
4/22/15	FY14-FY17	Removed OMB headings (ex. AXXA) from headings for entire document	

Document Purpose

This purpose of this document is to describe the strategy for acquiring and managing IT within the U.S. Department of Education (The Department) to support the achievement of the strategic plan goals. There are five sections that discuss different aspects of implementing and managing IT resources. These five sections are as follows:

Section 1 Specifies the Chief Information Officer's (CIO) objectives and planning horizon of the Information Resources Management (IRM) Strategic Plan. The Introduction also provides an overview of the external policies incorporated in the Department's IRM Strategic Plan.

Section 2 Identifies the strategic goals set by the CIO to achieve the Department's technology objectives.

Section 3 Describes Goal One of the Department's IT portfolio alignment. This section discusses how the portfolio is aligned to meet the Department's business mission and Federal IT initiatives.

Section 4 Describes Goal Two of the Department's IT portfolio alignment. This section identifies the current technology services offered at the Department, along with future technologies that will meet the Department's growing business requirements.

Section 5 Describes Goal Three of the Department's IT portfolio alignment. This section identifies the key stakeholders and provides an overview of what they manage and contribute to the information resource management process.

1 Introduction

The CIO at the Department has primary responsibility to ensure that IT is acquired and information resources are managed in a manner consistent with statutory, regulatory, and departmental requirements and priorities. The CIO provides management advice and assistance to the Secretary of Education and to other senior staff on information resources investment and operations. The CIO also promotes a shared corporate vision for the Department's information activities, and provides services to effectively manage information, while providing value-added, enterprise-wide systems and infrastructure.

The Department Information Resources Management Strategic Plan for FY 2014 - 2017 describes:

- The relationship between the IT vision and the enterprise business goals and performance objectives
- The set of value-added IT services delivered or planned to be delivered
- The set of IT management processes and plans for ensuring the effective use of IT resources across the Department

While the IRM Strategic Plan serves as the strategic document for the Office of the Chief Information Officer (OCIO), it is built from other more detailed strategic, operational and tactical plans of each information management element throughout the Department, ranging from enterprise architecture to E-Government. The IRM Strategic Plan describes what will be implemented over the planning horizon, while the other strategic, operational and tactical plans describe how these goals will be accomplished. Together, these plans allow OCIO to ensure that IT activities are aligned with, and supportive of, the Department's mission and strategic goals.

In addition, the Department recognizes the need to integrate external policies and directions as defined by Congress and the Administration into its IRM Strategic Plan. As such, the Department's IRM Strategic Plan responds to:

- Federal Information Technology Acquisition Reform Act (FITARA)
- Federal Information Security Management Act (FISMA)
- Clinger-Cohen Act of 1996
- E-Government Act of 2002
- Government Performance and Results Act of 1993
- Office of Management and Budget (OMB) Circular A-130
- Implementing PortfolioStat Memorandum OMB M-12-10
- Chief Information Officer Authorities Memorandum OMB M-11-29
- Federal Enterprise Architecture (FEA)

OMB Circular A-130 describes the IRM Strategic Plan as a management tool that is "strategic in nature and addresses all information resources management activities of the agency and agencies must develop and maintain the agency's IRM strategic plan" It also requires that the IRM Strategic Plan be submitted together with the Department's IT budget request.

2 IRM Goals

The CIO's objective is to support the Department's mission through effective management of value-adding technologies. The IRM Strategic Plan describes the technology strategic goals necessary to achieve the CIO's objective.

Figure 1: IRM Strategic Plan Goals

3 Goal One: Portfolio Alignment

Goal One of the Department's IRM Strategy is to ensure that the IT investment portfolio supports the Department's business mission objectives while delivering business value. The IT portfolio objective is to accomplish:

- Alignment to Departmental Business Mission
- Alignment to Federal IT initiatives

The IRM Strategic Plan describes how the Department's technology investments are managed to support the business mission and performance objectives of the Department's program offices, and to respond to Federal IT initiatives.

3.1 Department Alignment

The Department's IRM Strategic Plan is designed to demonstrate how the Department's information resources are aligned to support achievement of the Department's mission.

3.1.1 Department Strategic Plan

OCIO's technology goals are to support the achievement of the Department mission and strategic performance goals and objectives for 2014 – 2018.

The **Department of Education's mission** is:

> "To promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access."

The Department's Strategic Plan 2014-2018 embodies six Department of Education strategic goals:

Table 1: Department of Education Strategic Goals and Objectives

Strategic Goals	Strategic Objectives
Goal One: Postsecondary Education, Career and Technical Education, and Adult Education. Increase college access, affordability, quality, and completion by improving postsecondary education and lifelong learning opportunities for youths and adults.	Strategic Objective 1.1: Access and Affordability. Close the opportunity gap by improving the affordability of and access to college and/or workforce training, especially for underrepresented and/or underprepared populations (e.g., low-income and first-generation students, English learners, individuals with disabilities, adults without high school diplomas, etc.). Strategic Objective 1.2: Quality. Foster institutional value to ensure that postsecondary education credentials represent effective preparation for students to succeed in the workforce and participate in civic life. Strategic Objective 1.3: Completion. Increase degree and certificate completion and job placement in high-need and high-skill areas, particularly among underrepresented and/or underprepared populations. Strategic Objective 1.4: Science, Technology, Engineering, and Mathematics (STEM) Pathways. Increase STEM pathway opportunities that enable access to and completion of postsecondary programs.
Goal Two: Elementary and Secondary. Improve the elementary and secondary education system's ability to consistently deliver excellent instruction aligned with rigorous academic standards while also providing effective support services to close achievement and opportunity gaps, and ensure all students graduate high school college- and career-ready.	Strategic Objective 2.1: Standards and Assessments. Support implementation of internationally benchmarked college- and career-ready standards, with aligned, valid, and reliable assessments. Strategic Objective 2.2: Effective Teachers and Strong Leaders. Improve the preparation, recruitment, retention, development, support, evaluation, recognition, and equitable distribution 7of effective teachers and leaders. Strategic Objective 2.3: School Climate and Community. Increase the success, safety, and health of students, particularly in high-need schools, and deepen family and community engagement. Strategic Objective 2.4: Turn Around Schools and Close Achievement Gaps. Accelerate achievement by supporting states and districts in turning around low-performing schools and closing achievement gaps, and developing models of next generation high schools. Strategic Objective 2.5: STEM Teaching and Learning. Increase the number and quality of STEM teachers and increase opportunities for students to access rich STEM learning experiences.
Goal Three: Early Learning. Improve the health, social-emotional, and cognitive outcomes for all children from birth through 3rd grade, so that all children, particularly those with high needs, are on track for graduating from high school college- and career-ready.	Strategic Objective 3.1: Access to High-Quality Programs and Services. Increase access to high-quality early learning programs and comprehensive services, especially for children with high needs. Strategic Objective 3.2: Effective Workforce. Improve the quality and effectiveness of the early learning workforce so that early childhood educators have the knowledge, skills, and abilities necessary to improve young children's health, social-emotional, and cognitive outcomes. Strategic Objective 3.3: Measuring Progress, Outcomes, and Readiness. Improve the capacity of states and early learning programs to develop and implement comprehensive early learning assessment systems.

Strategic Goals	Strategic Objectives
Goal Four: Equity. Increase educational opportunities for underserved students and reduce discrimination so that all students are well-positioned to succeed.	Strategic Objective 4.1: Equitable Educational Opportunities. Increase all students' access to educational opportunities with a focus on closing achievement gaps and remove barriers that students face based on their race, ethnicity, or national origin; sex; sexual orientation or gender identity or expression; disability; English language ability; religion; socioeconomic status; or geographical location. Strategic Objective 4.2: Civil Rights Compliance. Ensure educational institutions' awareness of and compliance with federal civil rights obligations and enhance the public's knowledge of their civil rights.
Goal Five: Continuous Improvement of the U.S. Education System. Enhance the education system's ability to continuously improve through better and more widespread use of data, research and evaluation, evidence, transparency, innovation, and technology.	Strategic Objective 5.1: Data Systems and Transparency. Facilitate the development of interoperable longitudinal data systems for early learning through employment to enable data-driven, transparent decision making by increasing access to timely, reliable, and high-value data. Strategic Objective 5.2: Privacy. Provide all education stakeholders, from early childhood to adult learning, with technical assistance and guidance to help them protect student privacy while effectively managing and using student information. Strategic Objective 5.3: Research, Evaluation, and Use of Evidence. Invest in research and evaluation that builds evidence for education improvement; communicate findings effectively; and drive the use of evidence in decision-making by internal and external stakeholders. Strategic Objective 5.4: Technology and Innovation. Accelerate the development and broad adoption of new, effective programs, processes, and strategies, including education technology.
Goal Six: U.S. Department of Education Capacity. Improve the organizational capacities of the Department to implement this strategic plan.	Strategic Objective 6.1: Effective Workforce. Continue to build a skilled, diverse, and engaged workforce within the Department. Strategic Objective 6.2: Risk Management. Improve the Department's program efficacy through comprehensive risk management, and grant and contract monitoring. Strategic Objective 6.3: Implementation and Support. Build Department capacity and systems to support states' and other grantees' implementation of reforms that result in improved outcomes, and keep the public informed of promising practices and new reform initiatives. Strategic Objective 6.4: Productivity and Performance Management. Improve workforce productivity through information technology enhancements, telework expansion efforts, more effective process performance management systems, and state-of-the-art leadership and knowledge management practices.

Source: U.S. Department of Education Strategic Plan 2014-2018

3.1.2 Segment Architecture

The OCIO's Enterprise Architecture Program Office (EAPO) developed a Segment Architecture approach to align the IT portfolio to the Departmental strategic goals.

The EA Program Office, in accordance with the FEA practice guidance, identified business segments that support common missions and provide common services. These business segments are then grouped into categories by how they address the various business and technology needs of the program and principal offices across the Department: core mission, business service, and enterprise services. As a

result of the identification and development process, the EA Program Office described the Department's business using the 13 segments in the following table.

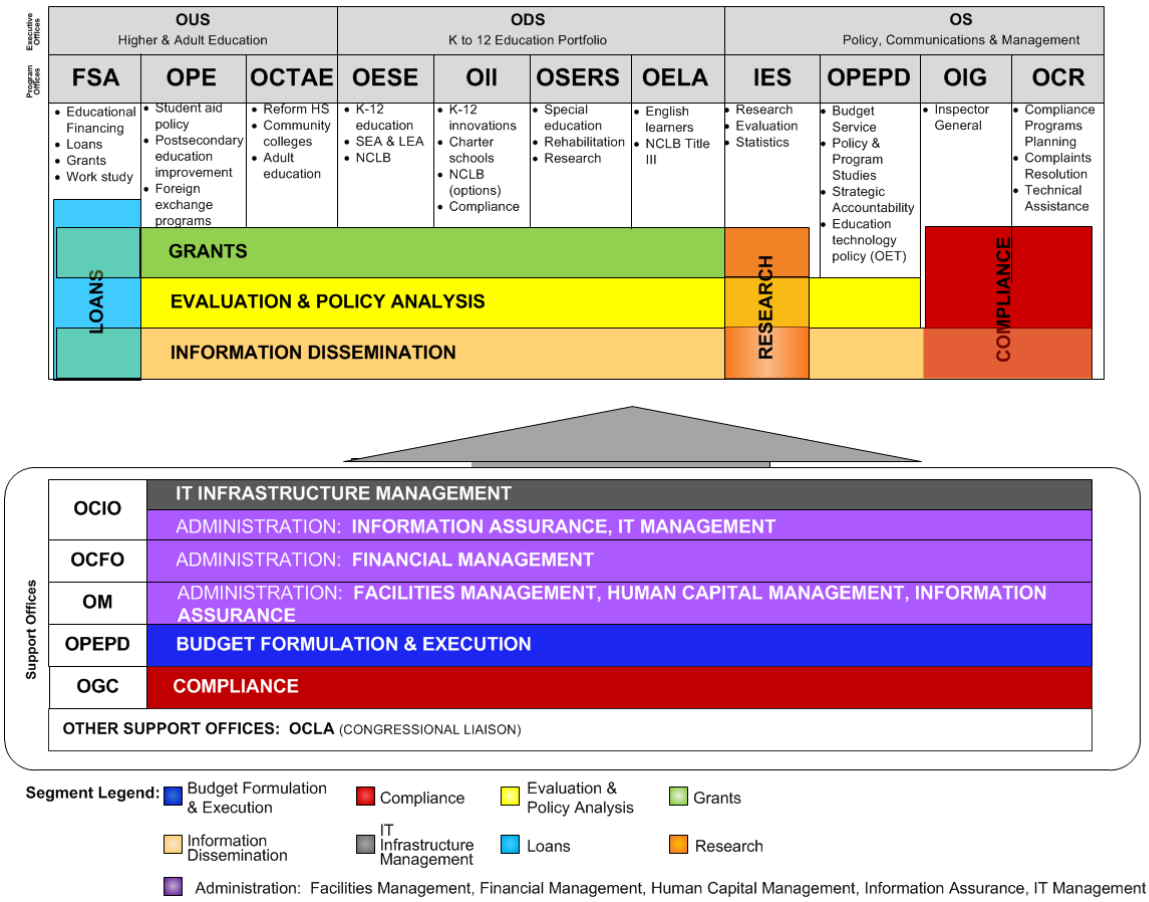
Table 2: The Department's 13 Segments

Segment Name	Segment Definition	Segment Category
Budget Formulation & Execution	Enable the Department's budget personnel to reduce manual processes and improve budget formulation and execution efficiency and data accuracy	Business Service
Compliance	Ensure that policies mandated by the Department and by Federal law are being carried out	Core Mission
Evaluation & Policy Analysis	Assess the Department's programs and related policies for meeting national education objectives	Core Mission
Facilities Management	Track assets and the provision of services related to those assets, to include the operation of office buildings, space planning, and other capital assets that are possessions of the Department	Enterprise Service
Financial Management	Deliver responsible financial management capabilities, including centralized data, increased access, electronic record keeping, and improved reporting	Business Service
Grants	Review, award, and disbursement of formula and discretionary grants through the various program offices	Core Mission
Human Capital Management	Improve the strategic management of the department's human capital	Business Service
Information Assurance	Build and enable mutual trust needed to support widespread use of electronic identity authentication interactions between the public and the government	Enterprise Service
Information Dissemination	Distribute education information products through multiple channels and formats	Core Mission
IT Infrastructure	Improve customer service and reduce the Department's operational risks by improving performance, providing a common technology platform for business applications, and facilitating better information management	Enterprise Service
IT Management	Facilitate the interagency-wide governance of information resources, to include the practices of enterprise architecture, and capital planning and investment control	Enterprise Service
Loans	Manage and deliver federally funded or federally guaranteed financial assistance for post-secondary education	Core Mission
Research	Research and statistical analysis on the condition of education in the U.S.	Core Mission

The EAPO worked with the segments to establish the investments in the Department's IT portfolio and how they were developed to improve the business performance of the program offices they support.

The following figure provides a visual representation of principal offices and their engagement with the Department's 13 Segments.

Figure 2: Principal Office and Segment Engagement



The segment architecture approach is expected to improve the Department's performance and help identify ways to reduce cost by aligning business processes and investment activities while eliminating unnecessary duplication of processes, investments and technologies.

3.1.3 Value Measurement Methodology (VMM)

The VMM is the process that is used to assess the relative value of the Department's IT investments. The VMM applies a numerical scale to the Department's mission priorities, value drivers and performance metrics to assign a value score to each of the Department's IT investments. The VMM value score is combined with other rating factors such as the CIO ratings and Planning and Investment Review Working Group (PIRWG) select scores to make funding and management decisions about the Department's IT investment portfolio.

The PIRWG uses the VMM in the portfolio selection process to make funding recommendations about IT investments and IT investment opportunities. The segment owners of the Department's lines of business (LOB) use VMM to make IT investment planning decisions and determine their priority and funding recommendations to the PIRWG about those IT investments. The VMM also helps the

Department identify opportunities for investment consolidation and/or termination, thereby increasing the efficiency of IT services and resource utilization by the Department.

3.2 Federal Alignment

The Department's goal to align its portfolio also includes alignment to Federal technology initiatives.

By implementing the following initiatives in compliance with government-wide mandates, the IT portfolio will support the Federal government's technology direction:

- Digital/Open Government Strategy
- EA Value
- ED Space Modernization
- Customer Service
- Cloud Computing
- Homeland Security Presidential Directive (HSPD-12)
- Investment Consolidation
  - Financial Management
  - Grants Management
  - Website Consolidation
- Trusted Internet Connection (TIC)
- Electronic Stewardship
- Performance Measurement

On May 23, 2012, the White House released its strategy for digital government, "Building a 21st Century Platform to Better Serve the American People." The strategy has three primary objectives:

(1) Enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device

(2) Ensure that as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways

(3) Unlock the power of government data to spur innovation across our Nation and improve the quality of services for the American people

Four overarching principals drive this digital government transformation:

(1) An "***Information-Centric"*** approach – Transforming from managing "documents" to managing discrete pieces of open data and content, which can be tagged, shared, secured, mashed up and presented in the way that is most useful

(2) A ***"Shared Platform"*** approach – Enables the government to work together, both within and across agencies, to reduce costs, streamline development, apply consistent standards, and ensure consistency in how the Department creates and delivers information

(3) A ***"Customer-Centric"*** approach – Influences how data is created, managed, and presented through websites, mobile applications, raw data sets, and other modes of delivery, and allows customers to shape, share and consume information, whenever and however they want it

(4) A platform of ***"Security and Privacy"*** – Ensures this innovation happens in a way that ensures the safe and secure delivery and use of digital services to protect information and privacy

The Department is committed to supporting the digital government strategy through the engagement in the action plan presented in the following table.

Table 3: Department Action Plan

Digital Government Strategy Principal	Departmental Action Plan Activity
Information Centric Approach	• Engage with customers to identify major customer-facing services that contain high-value data or content to make compliant with new open data, content, and web API policy • Make open data, content, and web APIs the new default by ensuring all new IT systems follow the open data policy and operationalize ED.gov and developer pages • Publish a plan to transition additional high-value systems to make high-value data and content in existing major customer-facing systems available through web APIs and metadata tagging
Shared Platform Approach	• Establish an agency-wide governance structure for developing and delivering digital services • Develop an enterprise-wide inventory of mobile devices and wireless service contracts • Evaluate the government-wide contract vehicles in the alternatives analysis for all new mobile-related procurement
Customer Centric Approach	• Engage with customers to identify existing priority customer-facing services to optimize for mobile use • Ensure all new digital services follow digital services and customer experience improvement guidelines • Optimize two existing priority customer-facing services for mobile use and publish a plan for improving additional existing services • Implement performance and customer satisfaction measuring tools on all government websites
Platform of Security and Privacy	• (Via CIO Council) Evaluate opportunities to accelerate the secure adoption of mobile technologies into the federal environment at reduced cost • (Via CIO Council) Develop guidelines for standardized implementation of digital privacy controls and educate agency privacy and legal officials on options for addressing digital privacy, records retention, and security issues

3.2.1 Digital Government Strategy

3.2.1.1 Implementing the Digital Government Strategy

The Department of Education's approach to the Digital Government Strategy focuses on:

- Better serving the Department's customers
- Sharing ideas, solutions, and best practices across the Department
- Offering more cohesive processes for the delivery of digital services

- Ensuring cost effective delivery of services
- Ensuring digital services provide value
- Reducing redundancies in digital services and data collections across the Department

The Department's Data Strategy Team (DST) is conducting an inventory of all public and restricted datasets, and is studying ways to build more coordinated policies and processes for data collection and release throughout the information life cycle across the Department. The DST has established a Disclosure Review Board led by the Department's Chief Privacy Officer. The Department's Digital Government Strategy working group plans to propose revisions to the Department's Lifecycle Directive Framework (OCIO 1-106) policy document and to standard language for contracts and statements of work to promote interoperability and data openness for new and renewed IT systems.

The Department has engaged with the broader education community and other interested developers and entrepreneurs through social media outlets and the Department's official Homeroom Blog. Blog visitors have the opportunity to comment on the blog post and provide feedback about services and data they would like to access through open web APIs. Representatives from the Department's OCIO, the Office of Communications and Outreach, and other key offices collect, analyze, and synthesize the feedback from the blog and social media comments to prioritize the development of APIs. The Department's White House Innovation Fellow is engaged in the Project Open Data initiative, and the Department had made its data inventory available as a JSON file to ensure its data publication workflow will be compatible with the new implementation approach for Data.gov.

3.2.1.2 Information Centric

3.2.1.2.1 Open Government Directive

The December 2009 Open Government directive set an unprecedented standard for openness in government. Open Government practices became an even more prominent priority at the Department with the issuance of the President's Open Government directive, Transparency and Open Government, on January 21, 2009.

The Department's Open Government Plan articulates Secretary Arne Duncan's response to the Office of Management and Budget's Open Government Directive (OMB M-10-06). The directive requires departments and agencies to document specific steps that will achieve the transparency, participation, and collaboration goals of President Obama and his administration.

The goals of Open Government are to:

Table 4: Open Government Goals

Goals	Objectives
Increase the Department's transparency and accountability.	• Provide clarity and guidance on privacy rules and regulations to ensure that information and data can be shared in a timely manner with the public while still protecting individual privacy as required by law. • Make more data and information available to the public. • Improve the timeliness of Freedom of Information Act (FOIA) processing and document release. • Increase the transparency of the grant application and award process. • Maintain up-to-date information on the Department's website about Department offices and key programs. • Foster more transparency in the larger educational community.
Solicit and incorporate more public input, including from students, families, educators, and community partners, into Department operations and programs.	• Provide more insight into the agency's decision-making process. • Provide regularly updated project maps, dated milestones, and financial data regarding open government and other key initiatives. • Collect and use input from the public and other stakeholders, including students, families, educators, and community partners, in decision-making. • Empower students, families, educators, and community partners to have a voice in the development and implementation of Department-funded education projects at the state and local level.
Increase collaboration and communication with other organizations.	• Enhance collaboration with other federal and non-federal agencies, the public, and non-profit and private entities.
Create a culture of openness within the Department.	• Encourage openness and communication about effectiveness within the Department. • Enhance Departmental internal collaboration capabilities.

3.2.1.2.2 Open Data

The Department formed a DST representing all the Department's offices that work with data collections to coordinate data-related policy activities within the Department. The DST established a number of working groups pertaining to various data-related initiatives within the Department, developing or redesigning policy, processes, and/or tools. Among them, DST established the Data Inventory Group (DIG), tasked with developing a database of information about all Department-sponsored data collections that can be used to produce education statistics. The primary purpose of the database is to provide a centralized searchable source of background information about the Department's collections, with the goal of facilitating both internal and external awareness of available data, and increasing data use and coordination among current and future data collections.

DIG members met first as a group and then worked via email to determine the type of background information (metadata) to collect, and to identify the initial scope of the group's product. DIG members agreed that as a starting point, any data collection that has an OMB clearance would be included in the

inventory database, encompassing both Department-sponsored data collections and reporting requirements for Department-sponsored grants. The database is currently being populated using the electronic OMB clearance packages (i.e., those submitted for clearance since 2005). To date, metadata for 46 program areas, big and small (including EdFacts and many NCES studies), have been entered into the ED data inventory database based on 269 OMB clearance packages. That is, and can be viewed, at data.inventory.gov.

3.2.1.2.3 Data.gov

As part of the Open Government Initiative, Data.gov shares the Open Government initiative's goals to increase agencies' transparency and accountability with the public by providing improved access and usability of Federal data.

Additionally in FY2012, OMB, General Services Administration, the Department and other federal agencies with education-related data (e.g., National Science Foundation, National Aeronautics and Space Administration, Veterans Affairs, U.S. Department of Agriculture, U.S. Department of State), launched the Data.gov Education Community at http://education.data.gov. This website showcases education-related datasets, challenges, mobile and web applications and other interests to the community.

Data.gov and Data.ED.gov are user-friendly platforms with a searchable data catalog that makes more data and information available to the public and also provides regular updates to project maps, dated milestones, and financial data regarding Open Government and other key initiatives. These Data.gov programs provide the public with increased access to high value, machine readable datasets so that they can easily find, download, and use information generated by the Department.

3.2.1.3 Shared Platform

3.2.1.3.1 Cloud Computing

The February 2011 Cloud Computing Initiative and the Federal Cloud Computing Strategy require all Federal agencies to shift to a "Cloud First" policy. The goal is to become a more reliable, efficient, and innovative government.

The Department of Education is adopting cloud computing technologies whenever a secure, reliable, cost-effective cloud option exists in compliance with the following guidance and regulations:

- Federal Chief Information Officers Council (FCIOC) Privacy Committee, Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies, August 2010
- FISMA of 2012, Public Law 104-347
- NARA Bulletin 2010-05, Guidance on Managing Records in Cloud Computing Environments
- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011
- NIST SP 800-145, A NIST Definition of Cloud Computing, September 2011
- NIST SP 800-146, DRAFT Cloud Computing Synopsis and Recommendations, May 12, 2011

- OMB Circular A-130
- The Cloud Computing Act of 2011
- The Federal Risk and Authorization Management Program (FedRAMP)
- Department of Education Cloud Computing Strategy, September, 2014

3.2.1.3.2 Shared Services

The Department's shared services strategy addresses the Federal Information Technology Shared Services Strategy, which provides policy guidance on the full range and lifecycle of intra- and inter-agency IT shared services. This strategy is part of the OMB "25-Point Implementation Plan to Reform Federal IT Management," which seeks to increase return on investment, eliminate waste and duplication, and improve the effectiveness of IT solutions. The approach is commonly referred to as the "Shared-First" strategy.

The Department's shared service plan also seeks to comply with the following guidance:

- OMB Memorandum M-11-29, Chief Information Officer Authorities, August 8, 2012
- OMB Memorandum M-12-10, Implementing PortfolioStat, March 30, 2012

Please see Section 4.2.3 for more information on the Department's shared services activities.

3.2.1.3.3 Investment Consolidation

Investment consolidation has been identified as a new initiative for the Department. Currently, it is comprised of three major components: Financial Management Consolidation, Grants Consolidation, and Web Consolidation (moving all Department websites to the same platform). The purpose of this consolidation is to begin to aggregate data onto the same platform to help increase access, use, and interoperability.

Currently, the following three non-major Financial Management Segment investments which are considered to be key financial applications are not included as part of Educating Central Automated Processing System (EDCAPS) architecture and are therefore not in either the Financial Management Support System (FMSS) or the Integrated Support Service (ISS) investment. Through investment consolidation, these three investments (key financial applications) will be included under the EDCAPS umbrella and, if feasible, managed within the FMSS:

(1) Frontier (formerly CheckFree RECON Plus for Windows)

(2) Continuous Controls Monitoring System (CCMS)

(3) Interface between Internet Payment Platform (IPP) and Oracle.

The proposed grants consolidation initiative is an effort to ensure the Grants Management system (G5) is the definitive, integrated grant-making platform that addresses the business needs of all grants-making offices at the Department. This roadmap will outline a strategy for migrating existing functionality and systems into G5, enabling elimination of current IT investments or systems, and provide a path for new functionality requirements to be incorporated, as well. This effort will be completed in cooperation with the Office of the Chief Information Officer (OCIO), and the Grants

Executive Board (GEB). The GEB, which has representation from all grants-related organizations in the Department, will provide oversight and support of the grants consolidation intiaitve, while its members instruct their respective organizations on the tasks needed to complete the effort. This consolidation is going to streamline processing and decrease required processing time, while aggregating grants information allowing for increased productivity and user satisfaction.

With web consolidation, the Department has noticed that many ED websites do not utilize the provided ed.gov domain names. The Department has realized that this causes problems with both customer intereactions and availability. With Department websites not utilizing the provided ed.gov domains, there are issues with branding, inconsistent service, and increased costs due to multiple hosting facilities. The web consolidation effort attempts to migrate these sites onto the ed.gov platform ensuring consistent service and availability. Succeeding in this will provide a number of benefits for the Department such as better branding, increased security, accelerated modernization, decreased costs, and increased leverage of shared services.

3.2.1.4 Customer Centric

3.2.1.4.1 Customer Service

The Department's Customer Service Plan is designed to improve the delivery of services to our customers by redesigning the business processes and systems that impact key customer interactions, including increasing online services and user-friendly services. The Customer Service Plan also addresses the Executive Order 13571 – *Streamlining Service Delivery and Improving Customer Service* to improve the quality of service the Federal government provides to the public, private entities, and intra-governmental agencies.

The Department's Customer Service Plan FY 2012 outlines the Department's efforts to improve customer relationships and the customer experience by delivering faster and better services to the public while reducing costs. The Department is currently forming a working group with customer service representatives from across the enterprise to update and expand the current Customer Service Plan.

3.2.1.4.2 Electronic Stewardship

In support of Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance, the Department will continue to serve as an active member on the Federal Electronic Stewardship Working Group (FESWG) and other interagency activities, including the Federal Electronics Challenge. The Executive Order, released in October 2009, includes the following areas associated with IT electronic stewardship that the Department will continue to implement and address throughout the acquisition, operations and end-of-life management lifecycle:

- Establish and implement policies to enable power management, duplex printing and other energy efficient or environmentally preferable features
- Use environmentally sound disposal practices for excess or surplus electronic products
- Implement best practices in energy-efficient management of servers and data centers

The Department's Strategic Sustainability Performance Plan outlines the agency's electronic stewardship programs and complies with the following guidance:

- Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance
- Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management

Please see Section 4.2.8 for more information on electronic stewardship.

3.2.1.4.3 EA Value/Performance

In the next year, the EAPO will develop outcome-oriented EA metrics in order to improve EAPO effectiveness and more efficiently prioritize and manage EA resources and the IT portfolio. Traditional metrics approaches tend to fail in their effort to demonstrate EA impact on business objectives. Through the use of outcome-oriented EA metrics, EAPO will drive effective resource allocation and prove the value and performance of EA to the Department business executives and IT executives. The approach for developing these metrics will follow the model below:

Table5: EA Value Metrics

Step	Description
1. Identify ED Value Drivers	EA will work with senior leaders to identify ED-specific business value drivers which are distinct sources of value delivery. Those value drivers will provide EA with clear guidance on EA services and deliverables.
2. Define EA Services	Through analysis EA will differentiate EA services from EA enabling activities. EA services are consumable, replicable, and apply to a variety of circumstances. Additionally EA services are designed to directly support a specific objective.
3. Link Deliverables to EA Services and Value Drivers	The deliverables or outcomes that result from the EA enabling activities will be linked back to the EA services that are comprised by those activities, and the ED value drivers which guide those EA services.
4. Specify the Business Impact of each Deliverable	Through the consolidation of external benchmarks, internal process knowledge, and subject matter expertise, EA can begin to calculate the potential value of the outcomes. This will be supported through the development of questions that assess how each deliverable impacts the current state. That impact will be used to define relevant outcome-oriented metrics.
5. Define Metrics	The metrics are outcome-oriented and will provide quantifiable measures for IT cost savings, business value creation, EA compliance, EA environment, and EA activities.

3.2.1.4.4 ED Space Modernization

This initiative strives to bring a new approach to the workplace at the Department of Education, build greater employee performance and productivity through innovative space designs and technology enhancements, while reducing the agency's space footprint and associated out-year costs. This initiative aims to reduce the Departments footprint to between 150-180 sq/ft in compliance with new federal guidelines. The modernization will provide the Department such benefits as upgrades to the IT infrastructure, it strengthens performance management, designs innovative work spaces, reduces the Departments footprint, and provides 21st century tools to support a new mobile workforce. Most importantly, it provides the option for mobile computing and gives greater opportunities for hiring

mobile employees. This allows the Department to leverage talent from all over the country, not just from local markets.

This initiative is highly aligned with the Access Anywhere and Cloud strategy initiative to provide mobile access to the Department's data and applications.

3.2.1.5 Security and Privacy

3.2.1.5.1 Homeland Security Presidential Directive (HSPD) 12

The Federal government established the HSPD 12 - Policies for a Common Identification Standard for Federal Employees and Contractors, the requirement that users provide two forms of identification for access to government systems. This required a government-wide standard for secure and reliable forms of identification. Agency goals in the department-wide integration of HSPD-12 are to reduce identity fraud, protect personal privacy, enhance security, and increase efficiency.

Please see Section 4.2.6.1 for more information on the Department's HSPD-12 activities.

3.2.1.5.2 Identity Management

The Federal government is moving toward the idea of sharing credentials across multiple agencies and allowing citizens to use non-government credentials to conduct business with the government online. The Department has been a participant in the identity management initiative, which is part of the E-Government agenda outlined by the President's Management Council.

Identity management provides the capability for the Department's customers to use identity credentials other than those currently provided by the Department of Education, such as those from the top five identity providers: (1) banks, (2) universities, (3) Internet service providers, (4) merchants, and (5) employers.

The Department's identity management program seeks to provide identity credentials to the Department's customers while strengthening security, reducing inconvenience, and minimizing the cost of identity management.

The Department's approach to implementing identity management is to build a solid infrastructure that supports shared authentication services across multiple applications. The first building block is the security architecture infrastructure that includes identity and access management (IBM Tivoli Access Manager and Identity Manager suite of products). The security architecture provides tools, technologies, and policies for identity and access management across the Department. The goal is to provide consistent access control, authorization and auditing for applications that integrate with this infrastructure. Once the security architecture is developed and deployed, the identity management infrastructure can be layered on top of it and deployed to any application already in the security architecture.

3.2.1.5.3 Department ID and Access Control Implementation

To meet the requirement of HSPD-12, the Department's Office of Management Security Services provides policy to Department facilities in how to manage the vetting and credentialing of individuals requiring access to agency information systems and facilities. Having consistent policies in place reduces vulnerabilities to the Department's physical and logical assets.

The Department's HSPD-12 solution, the ID Card and Access Control System, is currently in place and is used by employees and contractors at the Department's headquarters and regional locations. All of these systems are networked to form one system. The ID Card and Access Control System also provides complete access control and alarm monitoring for sites, including the following additional features:

- Access Control
- Security
- Point Monitoring
- Elevator Control
- Photo ID Badges
- Guard Tour
- Key Tracking
- Image Recall with Historic and User Accountability Reporting
- Live CCTV display/control
- Interface with Paging, CCTV, Parking, Central Station Automated Alarm Systems, HVAC, and Elevator Control Systems

The Department maintains privately leased, GSA owned, or GSA leased facilities, all of which have staggered lease renewal dates. As facility leases expire, the determination of whether to relocate or to extend the present lease will be determined. Security systems for all locations must be 100% compatible with the existing systems for proper monitoring and access control.

3.2.1.5.4 Two-Factor Authentication

To improve the security and protect the assets of the Department, all employees and contractors are required to access authorized Department systems using two factor authentication. Two-factor authentication requires two authentication methods to access a system. At the Department, users are required to use their PIV-enabled identification badge and a Personal Identification Number (PIN) for access to the Department's network.

3.2.1.5.5 Trusted Internet Connection (TIC)

The Trusted Internet Connection (TIC) Initiative derives from the National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 and is the first of 12 initiatives in the President's Comprehensive National Cybersecurity Initiative (CNCI). The TIC Initiative aims to optimize and standardize the security of the Federal government's network connections.

The Department's TIC implementation will comply with the following OMB Memoranda:

- OMB Memorandum M-08-05, Implementation of Trusted Internet Connections
- OMB Memorandum M-08-16, Guidance for Trusted Internet Connection Statement of Capability Form
- OMB Memorandum M-08-26, Transition from FTS2001 to NETWORX
- OMB Memorandum M-08-27, Guidance for Trusted Internet Connection Compliance
- OMB Memorandum M-09-32, Update on the Trusted Internet Connections Initiative

Please see Section 4.2.6.2 for more information on the Department's TIC activities.

3.2.1.5.6 Internet Protocol Version 6 (IPv6)

Internet protocols (IPs) specify communication and interoperability rules on the Internet and on other IP networks. Internet Protocol version 4 (IPv4) is most widely used in current Federal network environments. With the exponential increase in demand across the global Internet community, IPv4's address space is nearing depletion, underscoring the need to transition to IPv6, which offers a larger Internet address space. OMB Memorandum M-05-22 mandates Federal agencies enable Internet Protocol version 6 (IPv6) within their current IPv4 networks.

The Department developed an IPv6 Transition Guide, which describes the Department's policies and activities to meet the Federal IPv6 requirements. The Department's IPv6 Transition Manager and IPv6 Working Group have met the FY2012 external application compliance milestones and have completed all of the FY2014 internal application compliance milestones as well.

Please see Section 4.2.7 for more information on the Department's IPv6 activities.

3.2.2 Federal Data Center Consolidation

The 2010 Federal Data Center Consolidation Initiative (FDCCI) called for a government-wide effort to consolidate Federal data centers with goals to:

- Promote the use of Green IT
- Reduce Federal costs
- Improve IT security posture
- Shift Federal computing to more efficient technologies

The Department of Education has achieved its data center consolidation target, completed an inventory of its data centers and related assets, and completed its targets of consolidation to two data centers.

Through data center consolidation, the Department aims to do its part to reduce Federal energy consumption, reduce operational costs, strengthen IT security, and move toward employing innovative and efficient technologies.

4 Goal Two: Technology Services

Goal Two is to orient OCIO as a provider of technology-based business solutions including infrastructure services.

OCIO will enable program offices to better focus on their mission competencies by providing a robust enterprise platform with technology services that:

- **Improve performance** by providing a highly capable communications and computing infrastructure

- **Improve efficiency** with interoperable technologies that can link work across independent tools and enhance staff productivity
- **Reduce costs** for IT service delivery by standardizing software and hardware platforms

4.1 Current Services

OCIO's role is to provide a stable technology infrastructure to support the business requirements of the Department. OCIO will continue the delivery of common IT resources, such as hardware, software, networks, and other services that support program offices business needs. OCIO will continue delivery of the following supportive technologies during the FY 2014 - FY 2017 IRM Strategic Plan.

Table 6: Current Delivery of Services

Hardware
Assistive technologies
Hardware infrastructure maintenance and upgrade
Software
Assistive technologies
Data Analytics
Data Management
Desktop Operating System – Upgrade to Windows 7
Email, Messaging, and Collaboration
Office Productivity Tools – Microsoft Office Suite 2010
Voice and Data
Network
Data Center
Data Warehouse
DNS SEC
Intranet
IPv4/ IPv6 Capable
Security
Servers
Services
Enterprise Architecture
IT Acquisition
IT Capital Planning
IV&V
Security (Authorization & Accreditation, Continuous Monitoring, HSPD-12, Remote Access)
Service Level Agreements

As OCIO delivers these common IT products and services to maintain a stable technology platform, it will also seek ways to improve productivity and cost performance by eliminating costly duplicative, legacy, and stand-alone systems.

4.2 Future Services

To prepare the Department to meet future business goals, OCIO's role will evolve to provide a broader set of technology services to the Department. This future direction will position OCIO to become a provider of enterprise common services beyond the current technical infrastructure.

OCIO continues to develop a clear design for the future enhanced set of service offerings and how these new services will be deployed, supported, and governed. What follows is OCIO's current thinking around what IT shared services will be offered based on the Department's business needs, and the management challenges that OCIO will need to address in the near future to provide these services in an effective and efficient manner.

The future core enterprise technology platform will improve the overall Department's productivity and fiscal performance with faster, more reliable, and more innovative technologies.

Management Structure for Future Services

The Department will focus on these key goals for the implementation of all future technology services:

- Establish an effective product and service delivery model
- Implement an effective governance model
- Support the programs to develop a funding strategy
- Provide superior IT services to the Department

The service delivery model for shared services will be based on the following set of guiding principles for OCIO's operating model:

- Promote a supplier-customer relationship between IT and the business units to foster a "customer service" culture in IT while maintaining the fiduciary role of OCIO
- Implement an appropriate funding model for shared services that promotes financial transparency so that customers understand the costs associated with the products/services they consume, and understand the cost levers available to them (e.g., accept a higher level of service for a higher cost to meet special business needs)
- Introduce a "product-centric" model that integrates multiple disciplines and ensures accountability for the products/services offered to the customers. This model would include future product strategy, service level options, product refresh plans, etc.
- Separate the product/service planning and development functions (plan/build) from the operations functions to allow each to excel in their own individual disciplines and ensure that strategic, tactical, and operational imperatives are met

The product and service model defines roles, responsibilities, and accountabilities for operating the shared services at the Department. Some of the management issues include:

- When should the Department come to OCIO for a service and when should the service be contracted-out?
- What is the role of OCIO in satisfying office-specific business needs and how does that role differ if the need is enterprise-wide?
- How can OCIO maintain its fiduciary role when another organization or entity delivers the shared service?
- How will the Department decide whether a shared service is to be provided by OCIO or another organization (e.g., Office of the Chief Financial Officer, Institute of Education Sciences)?
- What is the governance model that will address investment priorities, funding mechanisms, portfolio effectiveness, service levels for shared services, and adherence/compliance actions?
- Are there service-specific governance models that are required, i.e., shared applications require shared support functions and shared governance?
- What are the appropriate organizational and contractual vehicles that are required to deliver shared services?

Specific steps to move toward the shared services operating model include addressing the following:

- Understand and document the needs of the customers for specific products and services that can best be developed, delivered, and supported centrally
- Support the goals of Federal IT reform initiatives, such as Federal Information Technology Shared Services Strategy, the .GOV Reform Effort to Improve Federal Websites, and the Federal Mobility Strategy, using shared IT resources to the maximum extent possible
- Offer these shared products and services to the customer efficiently and at an appropriate level of service and cost
- Install product and service monitoring functions to adjust the product and service mix (i.e., specific products, services, new service levels, etc.) to reflect changes in the business needs and the demand for these products and services
- Define and adopt a sound management model that allows the organization to effectively address the strategic, tactical, operational, and governance issues simultaneously

4.2.1 CIO's Innovation Agenda

The CIO's Innovation Agenda identifies new technologies and services to generate cutting-edge business growth and advantage. The new technologies should be flexible and responsive to support ED's business operations with IT infrastructure, while offering new opportunities for growth.

The current focus of the CIO's Innovation Agenda is Access Anywhere Computing, which will integrate mobile computing into the Department's computing environment.

4.2.1.1 Access Anywhere Computing

The Department will make it easier for staff to work effectively inside and outside the office by making applications and data available on multiple platforms that are secure and accessible from anywhere, improving employee performance. By enabling employees to use their own devices to access data and allowing employees to collaborate together, the Department can improve employee efficiency and productivity. In addition, by allowing employees to use their own devices, the Department can reduce costs by freeing up agency IT resources, and by decreasing in-office space usage and overheads.

4.2.1.2 OCIO Support Services

To support the CIO's innovation agenda, OCIO offers the Department's business customers the following three technology support services:

- IT Governance and Planning Services
- IT Project Management Services
- End-user IT Support Services

IT Governance and Planning Services help program offices align their business priorities with enabling IT capabilities that support accomplishing the mission of both the Principal Offices and the Department. These services could include:

- Governance services that validate the requirements, design, implementation and performance for IT projects and/or the application of Common Enabling Services (CES) (e.g., workflow and collaboration tools) that solve specific business needs
- Program office IT planning services in support of multi-year IT investment and project plans that provide the maximum benefits of available IT resources to the office
    - These services could include future state IT visions for POCs, future state concepts of operation that identify the role of technical capabilities in supporting the business unit mission, and the development of transition strategies and project portfolios that leverage existing and new IT components

IT Project Management Services include a full range of services for applying technical capabilities to solve office business needs. These services are envisioned to involve custom application development services, package installation and deployment services, or individual subject matter expertise to support program office development teams (e.g., project management, acquisition guidance/support). These services could include:

- Applications development, enhancement and deployment services (e.g., web applications and decision support applications development)
- Commercial off the shelf (COTS) software package identification, selection, installation, and support
- IT solutions project management and acquisition support services

The selection and deployment of these services will require OCIO to engage in the following activities to provide IT solution development and deployment services:

- Develop detailed plans and product recommendations for various types of CES's
- Support program offices to define relevant knowledge work requirements that will be optimally fulfilled by the CES
- Acquisition, deployment, and operations of COTS products on the infrastructure to provide CES
- Develop common enterprise-wide solutions or custom-developed solutions for individual program offices
- Ongoing training, configuration support, help desk and related customer service top program office users to maintain or adjust usage of CES

End-user Support Services: The future direction for IT at the Department is heavily focused on data access and analytical activities in support of the Department's mission. With the exception of small pockets within certain organizations, the Department has little expertise in supporting its end users in these areas. As the Department moves toward the application of enterprise data stores, enhanced analytical tools for end users, and the rollout of common enabling infrastructure tools to its knowledge workers, these same knowledge workers will require support to effectively apply these new capabilities to their day-to-day efforts. A set of shared services will be provided to deliver this support to the end users and could include the following:

- End user data access, query and reporting support services, including Executive Dashboard support services, to ensure the users understand the data available to them, how to access that data, and how best to manipulate the data in performing sophisticated analyses
- Technology/solutions training and support services for end users so the users can effectively use the new capabilities and derive value from these investments

Enterprise application operations and end user support services (e.g., IES Support) involve the basic support for shared applications – efficiently delivered as a shared service. Applications that are shared across an organization require support that is also shared.

4.2.2 Common Enabling Services (CES)

OCIO regularly receives requests for new services that will improve the Department's business performance. Program offices, business units, and staff commonly requested the following technologies:

Table7: Common Enabling Services

Requested Service	Definition
Collaboration Management	Allow people to work together more efficiently by enabling greater information sharing
Data Analytics	The science of systematically applying proven qualitative and quantitative tools and methodologies to examine raw data for facts and relationships that lead to statistically sound, data-driven decisions. The Department wants to create a comprehensive Data Analytics program that includes Visualization, Data Governance, and Data Management.
Data Management	Usage, processing, and general administration of unstructured information
Electronic Document/Record/ Content Management	Control the capture and maintenance of the Department's documents and files
Mobility Tools	Tools that enable mobile computing
Report Management	Support the organization of data into useful information
Security and privacy	Tools that support confidentiality, integrity, and availability
Work Management	Allow the monitoring of activities within a business process

OCIO prioritizes its technology efforts by the most requested services from across the Department. Most of the Department's business units have requested collaboration management and electronic document/record/content management as enterprise services.

The Department funded an enterprise implementation of SharePoint to provide collaboration services. OCIO will continue to expand the use of the collaboration platform during FY 2014 – 2017.

Data Analytics is the science of systematically applying proven qualitative and quantitative tools and methodologies to examine raw data for facts and relationships that lead to statistically sound, data-driven decisions. The Department wants to create a comprehensive Data Analytics program that includes Visualization, Data Governance, and Data Management.

Collaboration management tools will allow Department employees to integrate and work together on a unified platform. A unified collaborative platform is the most effective way to connect people, processes, and information across the Department and will enable stakeholders to quickly adapt, scale and extend the platform in response to shifting business needs.

An electronic document/record/content management solution will allow the Department to control the capture and maintenance of an organization's documents and files. The availability of an electronic records management tool will provide quick and reliable information for decision making by developing standardized processes for classifying, storing, securing, archiving, and disposing of records.

The OCIO plans to provide SharePoint, Microsoft Office Productivity Suite, and HP TRIM as the collaboration management and electronic document/record/content management solutions to create the foundation for an enhanced enterprise technology platform.Using the proposed platform, the Department will be able to utilize the various technology services that are provided to create other automated business support applications. In FY-13, the Department implemented E-foldering in its G-5 system using HP Trim. Currently, E-Foldering is available to all grants programs. During FY14-FY17 we will expand this capability to the Contracting and Purchasing system (CPSS II).

The following **proposed enterprise technology platform** diagram illustrates the future vision of the enhanced enterprise technology platform followed by a table that links each requested enhanced service to the proposed technology that meets that need.

Figure 3: Proposed Enterprise Technology Platform

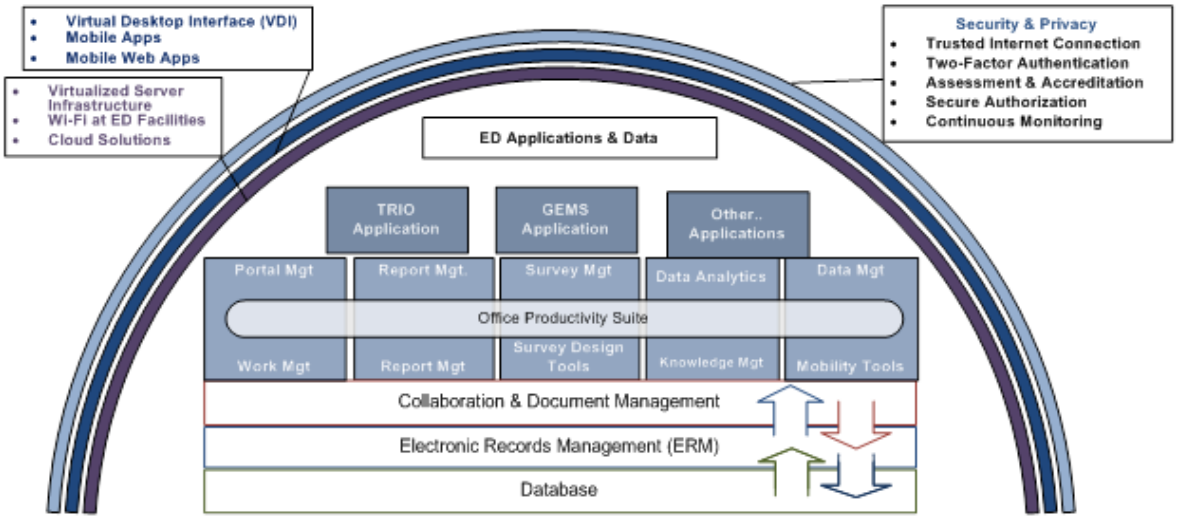


Table 8: Proposed Technology Solutions

Proposed Solution	Requested Service
Microsoft Office	Work Management, Mobility Tools, Survey Design Tools
Microsoft SQL Server	Data Management, Report Management
Microsoft SharePoint	Collaboration Management, Document/Record/Content Management, Survey Management, Portal Management
Microsoft OS Software	Security and Privacy, Mobility Tools
Microsoft Exchange, Outlook	Work Management, Knowledge Management, Data Management, Collaboration Management
Microsoft InfoPath	Report Management, Work Management, Knowledge Management, Data Management, Document/Record/Content Management
HP TRIM	Document and Records Management

4.2.3 Commodity IT and Shared Services

4.2.3.1 Maturing the IT portfolio

As part of the EA Roadmap, the Department has sought to optimize its IT infrastructure while operating an IT service management framework (primarily based on ITIL standards). The need for consolidation and use of shared services is identified through the segment modernization planning process. Modernization planning is an ongoing process, which uses performance objectives and business needs to determine if new investments or existing services should be utilized to meet the Department's business needs. During annual segment modernization planning, the segment owners review their line of business (LoB).

During annual segment modernization planning, each segment determines its required capabilities (currently met and unmet by existing investments) to achieve the segment's performance goals. The EAPO groups these needed capabilities into 18 common services. Additional details are provided in the Enterprise Modernization Roadmap.

4.2.3.2 *Use of savings resulting from consolidations of Commodity IT*

To date, the Department has successfully consolidated many enterprise services through the EDUCATE and Virtual Data Center (VDC) investments for (a) IT infrastructure; (b) Enterprise IT Systems; and (c) Business Systems. Moving forward, the Department has identified the following three major areas for consolidation:

- Financial Management systems
- Web Hosting, Infrastructure, and Content Management (Enterprise IT Systems)
- Grants-Related Federal Financial Assistance (Business Systems, for details, see the Commodity IT Consolidation Plan, an appendix of the Enterprise Modernization Roadmap)

The Department plans to use the savings obtained from using commodity IT to invest in performance-enhancing innovations within the Department.

4.2.3.3 *Maximizing use of inter- and intra-agency shared services*

Growing mission requirements in an environment of declining resources drives the Department to find innovative solutions to meet its needs. Shared IT services enable the Department to improve services and reduce overall costs, especially in areas of commodity IT, such as human resources, financial management, infrastructure, and business systems.

The Department aligns itself with the Federal Information Technology Shared Services Strategy, also known as the s*hared-first* approach. The shared-first approach aims to:

- Improve return on investment across the Department's entire IT portfolio through the coordinated use of portfolio reviews and commodity IT system and services consolidation
- Close productivity gaps by implementing integrated governance processes and innovative IT service solutions
- Increase communications with stakeholders as shared service managing partners, customers, and providers in the full lifecycle of IT shared service activities

Each system developed within the Department is reviewed by the Investment Review Board (IRB) for adherence to our IT value management and IT investment strategy. It is also reviewed by the Enterprise Architecture Review Board (EARB) for conformance with EA to ensure compliance with our technical standards, reduce the potential of acquiring duplicative investments and driving business value for IT investments.

As one of the smallest Cabinet-level agencies, the Department has historically operated an intra-agency shared IT services model for IT infrastructure, email services, office automation, networking, telecommunications and multimedia. Throughout its history, the Department has also leveraged the

products and services hosted by other agencies in lieu of maintaining Department systems for these services to drive cost efficiencies at the Department and Federal level. Most recently in October 2012, the Department moved from its internally hosted and developed "information collection" system to the Health and Human Services (HHS) http://www.paperworkreduction.gov portal for these services.

4.2.3.4 Continuity of operation for mission critical applications

Each system developed within the Department is reviewed by the EARB for adherence to numerous requirements, including continuity of operation and disaster recovery capabilities, consistent with documented Lifecycle Management Methodologies in Department directives and other Federal and Department regulations. In addition, the FISMA security authorization process evaluates systems as low, medium or high with respect to confidentiality, integrity and availability. Based on that analysis, applicable NIST Special Publication 800-53 controls will be required to provide a level of continuity of government operations.

4.2.4 Cloud Computing

The purpose of the Federal Cloud First policy is to move toward a more reliable, efficient, and innovative government. OCIO's cloud computing implementation will continue to modernize the Department's IT infrastructure with greater efficiency and improved virtualized technologies to support the Department's business performance.

During the FY 2014 - FY2017 IRM Strategic Plan, OCIO plans to provide the following cloud computing services:

Infrastructure-as-a-Service (IaaS): The Department will provide fundamental computing resources such as processing, storage and networks so that Department users can deploy and run software, operating systems and applications. IaaS will increase utilization of existing investments, reduce infrastructure investments and decrease IT expenses.

Platform-as-a-Service (PaaS): The Department will provide an integrated platform based computing solution on the cloud consisting of specific operating systems, applications software and development tools; that will be available via the Web. PaaS will improve the management and procurement of IT systems development capabilities.

Software-as-a-Service (SaaS): The Department will migrate some of its desktop software applications and data to the cloud infrastructure. The software is accessible from various client devices through a thin client interface, such as a Web browser. SaaS will improve the management, cost, and accessibility of software applications.

Additional migration of technology services to the cloud will be evaluated on an ongoing basis. These three cloud services will provide the Department's program offices and end-users with ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Table 9: Future Cloud Services

Service	Service Model	Deployment Model
Consolidated Web Hosting The Department is implementing a Web Consolidation policy that establishes a standard consolidated web hosting platform. This platform will be used to support the Department's information dissemination initiatives and require that website owners use the consolidated web hosting platform. The directive aims to consolidate the Departments information dissemination websites onto a common platform. This consolidation will ensure consistent branding and levels of security across all Department websites.	Iaas/ PaaS	Public Cloud
Enterprise Email in the Cloud The Department, in an effort to support the Access Anywhere initiative, has begun implementing Email in the Cloud. Currently, the staff of OCIO is migrated to the Cloud and the Department will migrate the remainder of the Department by FY17.	SaaS	Public Cloud
Collaboration Services (SharePoint) The Department plans on expanding its use of SharePoint and other collaboration tools.	SaaS	Public Cloud
IES Consolidated Platform IES is expanding their data center consolidation to the Cloud by moving the following items to the cloud by FY17: the Middle Grades Longitudinal Study (MGLS), Peer Review Information Management Online (PRIMO) system, the Regional Educational Laboratories (RELs), and will be implementing Sharepoint 2013 that will be used to house multiple sharepoint applications.	SaaS	Public Cloud
Office 365 The Department will move its Office Productivity tools into the Cloud. This will help the Department further conform to the Access Anywhere initiative.	IaaS	Public Cloud

4.2.5 Data Analytics Strategy Initiatives

A major focus of the CIO's innovation agenda is to develop and implement a data analytics strategy for the Department of Education. The CIO believes implementing this strategy will help create a data-driven culture that views Department data as a valuable asset that is used to make informed business decisions. The CIO expects that by implementing the data analytics strategy, the workforce efficiency, decision making, waste reduction and organizational productivity will improve.

4.2.5.1 Data Analytics at Department of Education

Data analytics is the science of systematically applying proven qualitative and quantitative tools and methodologies to examine raw data for facts and relationships that lead to statistically sound, data-driven decisions.

OCIO intends to implement data analytics in the Department. Data analytics will enable the Department's staff to improve business performance through the discovery of patterns, trends and facts in the data used to make effective business decisions that produces positive results. The data analytics process involves a series of steps that integrates, prepares, and transforms data into a structured format which can be used for data analysis and visualization.

4.2.5.2 *Creating a Data-Driven Culture at the Department of Education*

The CIO believes that, in order to build a data-driven organization that looks at data as an organizational asset to make informed decisions, there must be an internal cultural transformation within the Department. This organization-wide transformation will require the Department to review its processes, data governance, tools, people, and services holistically from a data and information perspective.

The four major areas identified by OCIO are:

1. Data Governance
2. People
3. Policies and Processes
4. Technology

4.2.5.3. Efforts at the Department to Establish a Data-Driven Culture

The Department is engaged in number of efforts to implement a data-driven culture within the organization.

4.2.5.3.1. Survey of Data Analytics Capabilities:

A survey of the 2015 Segment Modernization plans for the Department's business segments shows that many segments are currently using and have plans to expand their use of data analytics capabilities. This indicates there is a need for more data analytics capabilities in the Department going forward.

The following are some of the segments that are currently using data analytics capabilities within the Department:

Table10: Current Data Analytics Capability

Segment	Capability
Evaluation	Data Analysis, Visualization & Statistics
Compliance	Data Analysis, Visualization & Statistics
IT Management	Data Analysis, Visualization & Statistics
Loans	Data Analysis, Visualization & Statistics
Research	Data Analysis, Visualization & Statistics
Financial Management	Data Analysis, Visualization

4.2.5.3.2. Establish a Data Strategy Team (DST):

The DST was created by the Deputy Secretary to improve the coordination and approach to the collection, use and release of data. The DST consists of representatives from throughout the Department and is co-chaired by the Commissioner of the National Center for Education Statistics (NCES), the Chief of Staff of the Office of Planning, Education and Policy Development (OPEPD), and the Chief Privacy Officer (CPO) with support from OCIO.

The DST is responsible for the development, implementation, and coordination of data governance policy across all principle offices within Department.

4.2.5.3.3. Establish a Department of Education Data Governance Framework (ED-DGF)

The purpose of the Department of Education Data Governance Framework (ED-DGF) is to establish Department-wide roles and processes for managing data. The ED-DGF documents the Department's current data governance capabilities and addresses ways in which the current Data Governance structure can be adapted to better meet the Department's needs like the e-Information Collection Request datasets and datasets disclosed or released by the Department.

4.2.5.4. Data Analytics Technology

The CIO believes that to implement Data Analytics technologies in the organization, the technologies must be accessible, flexible, extensible, and integrated. Training on Data Analytics technologies must be provided to the Department staff to ensure they have the skill to leverage the use of these technologies to develop actionable insights from the data within the organization.

4.2.5.4.1. Data Analytics as a Service

To implement Data Analytics as a Service, as a first step, OCIO conducted a survey of the 2015 modernization plans of the business segments and has identified the following segments that are in need of "Data Analytics" capability:

Table 11: Segments requiring Data Analytics

Segment	Needed Capability
Evaluation	Statistical and Enterprise Analysis Tools (Expand RMS beyond risk analysis)
Financial Management	Statistical and Enterprise Analysis Tools
Grants Management	BI, Statistical and Enterprise Analysis Tools
Human Capital Management	Statistical and Enterprise Analysis Tools
Information Dissemination	Data Analytics and Visualization Tools
IT Management	Data Analysis and Visualization
Loans	Statistical and Enterprise Analysis Tools

Through the development of an enterprise-wide shared service platform, OCIO can provide data analytics capabilities as a shared services offering to Department's business segments. The segments can use, re-use, and combine the services to achieve a high level of data analysis capability and increase the Department's capacity while reducing the cost of ownership.

4.2.5.4.2. Future State- Services Oriented Architecture (SOA) for Data Analytics as a Service

To implement a Data Analytics as a Service capability, the Department must implement a flexible, scalable SOA to provide Data Analytics as a Service to its stakeholders.

SOA facilitates a loosely coupled, integrated, centralized, real-time, and open access to the organization's data and IT capabilities. Using an SOA, OCIO will be able to deliver data analytics services to the lines of businesses with increased agility, speed, and cost effectiveness.

4.2.5.4.3. Benefits of Implementing Data Analytics as a Strategy

The CIO understands that by adopting a flexible IT architecture design, OCIO can position itself as the organization that provides commonly used IT services such as Data as a Service to the business segments that require them.

The Department will implement a shared data analytics capability, based on SOA to transform the Department into a data-centeric organization. By implementing this strategy, the Department will effectively utilize its data, technology and human resources to improve its performance using data analysis, and create a strong data culture that values and manages data as an organizational asset to make business decisions.

**SLAs are contractual agreements between the provider and the customer that defines what constitutes as an acceptable service*

4.2.6 Cybersecurity Initiatives

OCIO's proposed enhanced enterprise platform will also accommodate the implementation of the following government-wide technology initiatives:

- Homeland Security Presidential Directive – 12 (HSPD-12)
- Trusted Internet Connection (TIC)
- Continuous Monitoring (CM)

The Federal government's technology initiatives are intended to lead government innovation while increasing business efficiency and fiscal responsibility.

4.2.6.1 HSPD-12

The Federal government established the 2004 mandate for HSPD-12 - Policies for a Common Identification Standard for Federal Employees and Contractors requiring a government-wide standard for secure and reliable forms of identification.

To meet the physical and logical access requirements of HSPD-12, the Department's top HSPD-12 agenda items are identity management, access control, and two-factor authentication. The Department's goals in the integration of HSPD-12 are to reduce identity fraud, protect personal privacy, enhance security and increase efficiency.

4.2.6.2 TIC

The TIC initiative aims to optimize and standardize the security of the Federal government's network connections. The Department's TIC implementation will improve the Department's security posture and incident response capabilities.

The Department received its Authority to Operate (ATO) as a Trusted Internet Connection Access Provider (TICAP) in January 2010. Most of the technology required has already been implemented in accordance with TIC 2.0. The technologies behind this capability provide improved situational awareness

and risk reduction to potential hacker, malware, malicious behavior, and data loss, as well as potential outages and negative public exposures caused by individuals, crime syndicates or state sponsored "hacker cells." The fulfillment of this requirement can be seen through blocking of Internet sites that are not in alignment with Department policies and existing rules of behavior, as well as protection from viruses and worms. Through proper handling of inbound and outbound email and implementing quarantine and junk mail filters, the Department minimizes other potential security issues via spear phishing attacks and the importing of malicious files.

The Department's current TIC efforts include activities to reduce and consolidate its external network connections, and enhance its external network monitoring capabilities. Forthcoming initiatives related to TIC are: secure email gateways, wireless networks, mobile computing and teleworking.

Continuous monitoring is provided directly via US CERT for the agency's Internet and external connections. This continuous monitoring provides critical situational awareness, oversight and coordination among all Federal agencies when dealing with attacks that directly target them.

The reduction and consolidation of Internet and external connections provides a smaller risk footprint to manage and oversee, as well as minimization of exposure risks.

The Department has also updated and deployed network and system warning banners to allow for improved prosecution of violators.

4.2.6.3 CM

OMB Memorandum M-11-33, FY 2011 Reporting Instructions for the FISMA and Agency Privacy Management, requires that all agencies develop a CM program. The Department's CM program is based on a phased-in maturity model approach. The phases align with the Continuous Monitoring Maturity Model found in the Continuous Monitoring and Risk Scoring (CM/RS) Concept of Operations (CONOPS) for Supporting Cyber Security Operations, as developed by the DHS Federal Network Security Branch. The Department is currently assessed to be at Maturity Level II with the implementation of some automated scanning tools and SCAP-compliant products. The Department intends to transition from Maturity Level II to Maturity Level V by FY 2017.

As part of the Department's ongoing transition to Maturity Level V, the Department is also maturing its enterprise-level Security Operations Center (EDSOC) to be the central point for operational IA/Cybersecurity situational awareness and reporting. The EDSOC will enable continuous and independent monitoring of the Department's cyber environment ensuring the protection and availability of IT assets and information. This effort will create an enterprise security operational capability to close the gaps and increase the ability of the Department to rapidly identify, respond to, mitigate, and proactively address vulnerabilities, incidents, and emerging threats. The scope also includes the build-out of a Sensitive Compartmented Information Facility (SCIF) at Potomac Center Plaza (PCP) for near, real-time access to classified information allowing the Department to detect, respond to, and mitigate threats and intrusions in a timely fashion.

4.2.7 IPv6

The Department has achieved its goal in transitioning to an IPv6 capable environment by achieving objectives perscribed by OMB in their 2012 and 2014 memos. As a result of these actions, IPv6 has provided enhanced technology services that improve the Department's business performance and operational efficiency. IPv6 enables the Department to support continued growth in users, devices and services that require internet-based functionality.

4.2.8. Electronic Stewardship

The purpose of the electronic stewardship program is to support the Federal leadership goals for economic, energy and environmental leadership as outlined in Executive Order 13514. Specific goals and activities supporting the agency's Strategic Sustainability Performance Plan include:

- 2014-2017: The Department continues to operate and maintain Energy Star and EPEAT Gold and Silver equipment, maintains power management settings, duplex printing and environmentally preferred purchasing of electronic equipment, and serves as a Federal champion for electronic stewardship. Additionally, the Federal Electronics Challenge has been replaced by the Federal Green Challenge, and the Department is evaluating its involvement.

5 Goal Three: Information and Technology Management

The IRM Strategic Plan's information and technology management goal is to ensure effectiveness of the Department's IT portfolio by fostering innovation, increasing IT portfolio value and enhancing cyber security.

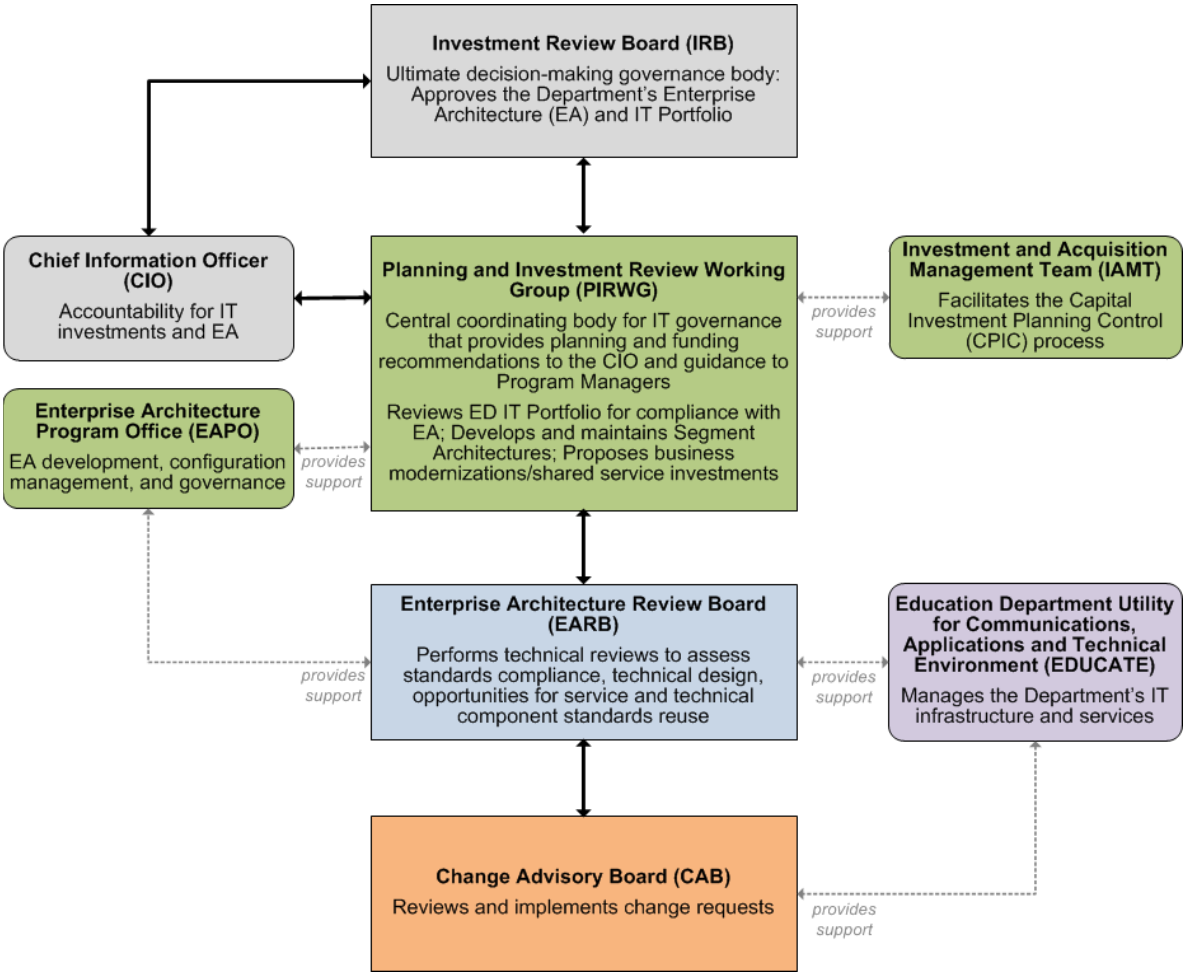
5.1 IT Governance Structure

The stakeholders in the Department's IT governance structure determine IT management policies and plans directly impacting the Department's information resources management process.

The Department's IT governance process is codified in Departmental Directive OCIO 1-106, Lifecycle Management (LCM) Framework. The LCM Framework provides the foundation for the implementation of standards, processes and procedures used in developing and managing technology. The Department's IT governance process ensures alignment of current and future IT initiatives to its strategic business objectives, as outlined in the FY 2014-2018 Department Strategic Plan.

The Department's IT governance process applies to major program/mission critical investments and non-major program/mission support investments that are included in the Department IT portfolio. The IT governance process ensures that the Department's IT portfolio is managed in a manner that is consistent with agency policy and OMB requirements. The IT governance process is managed through organizational entities – review boards and subordinate working groups shown the following figure.

Figure 4: The Governance Process at the Department



5.1.1 Enterprise Architecture Program Office (EAPO)

The EA Program Office is an essential component of the Department's IT governance process. The EA Program Office provides governance services, produces guidance and influences policies that directly impact information resources management.

The EA Program Office facilitates one governance process, the Enterprise Architecture Review Board.

- Enterprise Architecture Review Board (EARB): Provides support to PIRWG and EA Program Office by maintaining the Department's technical standards, ensuring standards compliance and interoperability, facilitating component reuse and validating solution architecture compliance with Department security standards

5.1.2 Investment and Acquisition Management Team (IAMT)

The Investment and Acquisition Management Team (IAMT) is an essential member of the Department's IT governance process. The IAMT ensures that all Department of Education IT acquisitions are reviewed

and accounted for in the Department's capital planning and investment IT portfolio. The IAMT supports the Department's information resources capital planning and investment control (CPIC) processes along with Department-wide bodies such as the IRB and the PIRWG to ensure continuity in the selection, monitoring, and evaluation of the Department's IT investments.

5.2 Key Department Contributors to the IRM Governance Process

The following Department programs are key contributors to the effective management of IT resources across the Department.

5.2.1 IT Acquisition (Procurement)

The Department's Contracts and Acquisition Management (CAM) team proactively leads the acquisition process, planning, negotiating, awarding and administering of contracts, including contracts for IT investments. CAM activities ensure the Department's procuring and contracting are completed in accordance with established Department and federal acquisition policies and procedures. CAM also provides a procurement career management program to ensure there is an adequate and professional acquisition work force at the Department. The Performance and Logistics Group, within CAM, provides technology, systems, acquisition policy and logistical support to Department groups.

5.2.2 Regulatory Information Management

Privacy, Information and Records Management Services (PIRMS) is the Department's organization responsible for providing policies, standards, and procedures that ensure the Department's activities comply with the Federal information management requirements.

5.2.3 Information Assurance Services (IAS)

Information Assurance Services (IAS) oversees the Department's IT security program and ensures the confidentiality/privacy, integrity, and availability of the Department's information and information resources. IAS ensures that the Department is fully compliant with FISMA and all related statutes and directives. The organization provides standardized security services and solutions in areas such as risk management, access controls, identity and access management, authentication, encryption solutions, public key infrastructure technology and certification and accreditation. The Department's Security Operations Center (EDSOC) enables continuous and independent monitoring of the Department's cyber environment ensuring the protection and availability of IT assets and information. This effort creates an enterprise security operational capability to close the gaps and increase the ability of the Department to rapidly identify, respond to, mitigate, and proactively address vulnerabilities, incidents, and emerging threats.

5.2.4 Information Technology Services (ITS)

Information Technology Services (ITS) supports all enterprise-wide initiatives that reside on the agency's network (EDUCATE) to include network security, network and telecommunications design and operations, end user services, production server hosting services and the agency's intranet and Internet

services. Additionally, ITS maintains and operates the Department's primary data center and disaster recovery facility. As assigned, ITS develops and maintains common business solutions that are required by multiple program offices. The ITS team manages or provides oversight for all enterprise-wide IT.

5.2.5 Accessibility

5.2.5.1 Creating a diverse work environment for individuals of all abilities

A key aspect of creating a diverse environment where individuals of all abilities can work, interact, and develop into leaders involves meeting the statutory requirements of Sections 504 and 508 of the Rehabilitation Act of 1973. These sections of the Rehabilitation Act protect and enhance the civil rights of individuals with disabilities throughout the country and ensure equality of opportunity, comparable access and improved quality of life for these individuals.

Creating a diverse work environment for individuals of all abilities involves the maintenance of a highly qualified, productive staff that has the necessary tools to perform work functions at its disposal. To ensure that staff with disabilities or impairments have the technology that provides them equal opportunities to perform alongside their non-disabled colleagues, OCIO conducts needs assessments and provides subsequent recommendations to EDUCATE. The recommendations of OCIO are aimed at providing adequate IT-related, "reasonable accommodations" to those employees who have functional limitations that warrant the application of assistive technology solutions. Such solutions, which include special keyboards for individuals with repetitive strain injuries, screen readers and magnifiers for the visually impaired, video phones for the deaf and hard of hearing, etc., mitigate the specific functional limitations of those individuals, thereby increasing job performance and enhancing involvement in all aspects of work life.

To make certain that all disabled employees and customers have full and complete access to the Department's information and systems, OCIO reviews whether web pages are sufficiently labeled, multimedia is adequately captioned, software controls are accessible with both the keyboard and the mouse, and documents are properly tagged, with good, readable-embedded text.

5.2.5.2 Building workforce skills to support and enforce Section 508 requirements

The Assistive Technology Team has held numerous training sessions for Department staff on a variety of topics, including the Section 508 standards, the document accessibility initiative, and accessible web design. The team has also conducted needs assessment awareness days, to familiarize staff members with their rights to receive assistive technology to assist in reducing or eliminating functional limitations they experience in the workplace.

Training on how to incorporate accessible document design into the day-to-day work process is currently being provided through the Training and Development Center, TDC on a regular basis to all Department staff. This is making a significant difference as POCS produce an increasing number of accessible documents.